IN THE CLAIMS

Please ~~add~~ claims 15-59 as follows:

15. (New) The PKVA of claim 1 wherein the registration authority does not maintain a certificate database.

16. (New) The PKVA of claim 15 wherein the table maintained by the credentials server is a hash table containing cryptographic hashes of valid issued unsigned PKVCs including a cryptographic hash of the first unsigned PKVC.

17. (New) The PKVA of claim 3 wherein the credentials server's response to the revocation request includes the credentials server ceasing to issue disposable PKVCs binding the subject's public key to the first PKVN.

18. (New) The PKVA of claim 17 wherein the credentials server's response to the revocation request includes the credentials server removing the table entry corresponding to the first unsigned PKVC.

19. (New) The PKVA of claim 17 wherein the PKVA's response to the revocation request includes the PKVA marking the first unsigned certificate in the certificate database as being invalid.

20. (New) The PKVA of claim 4 wherein the revocation request that includes the PKRC previously generated by the registration authority is sent to the PKVA; and the PKVA, upon receiving the subject's revocation request, verifies that the PKRC sent by the subject coincides with the previously generated PKRC.

21. (New) A method for managing the validity status of a subject's public key comprising:

issuing off-line to a subject a first unsigned public key validation certificate (unsigned PKVC) that binds a public key of the subject to a first public key serial number (PKVN);

maintaining a certificate database of unsigned PKVCs in which the first unsigned PKVC is stored;

issuing on-line to the subject a disposable public key validation certificate (disposable PKVC), that binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC; and

maintaining a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

Cl4 cont

22. (New) The method of claim 21 wherein the first PKVN is different than all previously-generated PKVNs.

23. (New) The method of claim 21 further comprising responding to a revocation request from the subject to invalidate the first unsigned PKVC entry in the maintained table.

24. (New) The method of claim 22 further comprising generating a public key revocation code (PKRC) to be used by the subject in the revocation request.

25. (New) The method of claim 23 further comprising sending the PKRC to the subject over a secure channel that provides data confidentiality.

26. (New) The method of claim 21 wherein the issued disposable PKVC includes an expiration date/time.

27. (New) The method of claim 26 wherein a validity period, from when the disposable PKVC is issued to the expiration date/time, is sufficiently short such that the disposable PKVC does not need to be subject to revocation.

28. (New) The method of claim 26 wherein the issued disposable PKVC is not subject to revocation.

29. (New) The method of claim 21 wherein the maintained table is a hash table containing cryptographic hashes of valid unsigned PKVCs stored in the certificate database and including a cryptographic hash of the first unsigned PKVC.

30. (New) The method of claim 21 wherein the disposable PKVC is issued in response to a message from the subject containing the issued first unsigned certificate.

31. (New) The method of claim 29 wherein the cryptographic hash of the first unsigned PKVC is computed with a collision-resistant hash function.

32. (New) The method of claim 31 wherein the collision-resistant hash function is a SHA-1 hash function.

33. (New) The method of claim 31 wherein the collision-resistant hash function is a MD5 hash function.

34. (New) The method of claim 21 wherein the issued disposable PKVC permits the subject to present the issued disposable PKVC to a verifier for authentication and for demonstrating that the subject has knowledge of a private key corresponding to the public key in the disposable PKVC.

35. (New) The method of claim 21 wherein a certificate database is not maintained.

36. (New) The method of claim 35 wherein the maintained table is a hash table containing cryptographic hashes of valid issued unsigned PKVCs including a cryptographic hash of the first unsigned PKVC.

37. (New) A public key infrastructure (PKI) comprising:
a subject; and

a first public key validation agent (PKVA) configured to maintain a record representing the status of validity of the subject's public key, the record has a high probability of being different from all other records of the first PKVA or of any other PKVA; and

a verifier configured to respond to an authentication of the subject, wherein the authentication includes ascertaining the validity of the subject's public key according to the record of the first PKVA.

A14 cont

38. (New) The PKI of claim 37 wherein the first PKVA is configured to bind the subject's public key to a first public key validation number (PKVN).

39. (New) The PKI of claim 38 wherein the first PKVN is substantially unique relative to all PKVNs previously used by the first PKVA.

40. (New) The PKI of claim 38 wherein the first PKVA is configured to issue a first certificate indicating the binding.

41. (New) The PKI of claim 40 wherein the first PKVA is configured to issue a second certificate indicating the validity of the subject's public key if the key has not been invalidated.

42. (New) The PKVA of claim 41 wherein the first PKVA is configured to respond to a request for invalidating the subject's public key, the first PKVA's response includes abstaining from issuing the second certificate.

43. (New) The PKI of claim 41 wherein the PKVA is configured to require the presentation of the first issued certificate in order to issue the second certificate.

44. (New) The PKI of claim 41 wherein the second certificate is a signed certificate.

45. (New) The PKI of claim 41 wherein the second certificate is a disposable certificate.

46. (New) The PKI of claim 45 wherein the disposable certificate is configured to expire after a selected passage of time.

47. (New) The PKI of claim 45 wherein the disposable certificate is configured to expire on a selected date/time.

a14 cont

48. (New) The PKI of claim 37 wherein the maintained record is keyed by a cryptographic hash.

49. (New) The PKI of claim 37 wherein the first PKVA is configured to respond to a request for invalidating the subject's public key.

50. (New) The PKVA of claim 49 wherein the responding includes verifying that the request was submitted by an entity having authorization to submit a request for invalidating the subject's public key.

51. (New) The PKVA of claim 50 wherein the responding includes requiring the presentation of a public key revocation code (PKRC) in order to invalidate the subject's public key.

52. (New) The PKVA of claim 51 wherein the responding includes verifying that the presented PKRC coincides with the previously generated PKRC.

53. (New) The PKVA of claim 49 wherein the responding includes altering the maintained record.

54. (New) The PKVA of claim 53 wherein the altering includes changing the validity status of the subject's public key.

55. (New) The PKVA of claim 53 wherein the altering includes removing the maintained record.

56. (New) The PKVA of claim 49 wherein the responding includes altering accessibility to the maintained record.

a14 cont

57. (New) The PKI of claim 37 further comprising a registration authority configured to authenticate the subject, the authentication comprises verifying that at least one purported identity attribute of the subject in fact applies to the subject.

58. (New) The PKI of claim 57 wherein the registration authority is configured to respond to an assertion of the validity of the subject's public key, the assertion is based on the record maintained by the first PKVA.

59. (New) The PKI of claim 57 wherein the registration authority is configured to certify the subject's authenticity, the certification includes the first PKVN, and an identifier of the first PKVA.